UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/811,177	03/26/2004	James F. Riordan	CH920020047US1	2029

48233 7590 09/16/2008

SCULLY, SCOTT, MURPHY & PRESSER, P.C.
400 GARDEN CITY PLAZA
SUITE 300
GARDEN CITY, NY 11530

EXAMINER	
TRUVAN, LEYNNA THANH	

ART UNIT	PAPER NUMBER
2135	

MAIL DATE	DELIVERY MODE
09/16/2008	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	10/811,177	RIORDAN, JAMES F.	
	Examiner	Art Unit	
	Leynna T. Truvan	2135	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *24 June 2008*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-23* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-23* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

1. Claims 3-5, 8-11, and 13-20 are pending.

Claims 1-2, 6-7, 12, and 21-22 are cancelled by applicant.

Continued Examination Under 37 CFR 1.114

2. A request for continued examination under 37 CFR 1.114, including the fee set forth in 37 CFR 1.17(e), was filed in this application after final rejection. Since this application is eligible for continued examination under 37 CFR 1.114, and the fee set forth in 37 CFR 1.17(e) has been timely paid, the finality of the previous Office action has been withdrawn pursuant to 37 CFR 1.114. Applicant's submission filed on 6/24/2008 has been entered.

Response to Arguments

3. Applicant's arguments with respect to claims 3-5, 8-11, and 13-20 have been considered but are moot in view of the new ground(s) of rejection.

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

4. *Claims* 3-5, 8-11, and 13-20 *are rejected under 35 U.S.C. 103(a) as being unpatentable over Ellison, et al. (US 7,236,956), and further in view of* Graunke, et al. *(5,991,399).*

As per claim 3:

Ellison discloses a method for detecting an attack on a data processing system, the method comprising, in the data processing system:

providing an initial secret; (col.7, lines 25-30)

binding the initial secret to data indicative of an initial state of the system (col.3, lines 52-65 and col.9, lines 4-7), which is installed on the kernel layer between a hardware layer and an operating system layer (col.2, lines 45-55 and col.3, lines 11-20), via a cryptographic function; (col.6, line 60 – col.7, line 5 and col.8, lines 38-60)

recording state changing administrative actions performed on the system in a log, the state changing administrative actions comprising one or more of: *[an installation of kernel modules and an alternation of system run-level codes];* (col.10, lines 43-65)

prior to performing each state changing administrative action, generating a new secret by performing the cryptographic function on a combination of data indicative of the administrative action and the previous secret, and erasing the previous secret; (col.9, lines 10-43 and col.11, lines 40-48)

evolving the initial secret based on the log to produce an evolved secret; comparing the evolved secret with the new secret; (col.11, lines 15-33 and 48-57)

determining that the system is uncorrupted if the comparison indicates a match between the evolved secret and the new secret; and (col.9, lines 45-55 col.11, lines 59-67)

determining that the system in corrupted if the comparison indicates a mismatch between the evolved secret and the new secret, (col.9, lines 55-60)

wherein the cryptographic function comprises a one-way hash function and the hash function comprises an exponentiation function. (col.9, lines 44-45)

Ellison teaches the invention includes an operating system with software modules such as the kernel that the processor nub loader is a protected bootstrap loader code held within a chipset in the system and records state changing administrative actions (col.3, lines 10-25). Although, Ellison suggests the protection of the operating system and kernel, however, Ellison did not clearly focus on kernel protection which fails to implicitly discuss the claimed recording state changing administrative action comprises an installation of kernel modules and an alternation of system run-level codes.

Teal teaches a system and method to verify the integrity of communications entering each individual computer resource in a computer network and thereby thwart unwanted or malicious intrusions into that portion

of an independent operating system resident in the kernel space of each computer resource in a computer network (col.1, lines 20-25 and col.3, lines 7-28). The invention includes computer code set which is loaded into the kernel where communication with which that portion of the operating system resident in the kernel space is checked by a computer code set installed in the kernel space. This is designed to detect and if necessary prevent the entry of unwanted or malicious programming code into that portion of operating system resident in the kernel space (col.8, lines 47-62). Teal further explains the operations and functions of loadable kernel modules and management of the kernel space on columns 13-15.

Therefore, it would have been obvious for a person of ordinary skills in the art to combine the teachings of Ellison with Teal to teach recording state changing administrative action comprises an installation of kernel modules and an alternation of system run-level codes because to thwart unwanted or malicious intrusions by detecting and preventing the entry of unwanted or malicious programming code into that portion of operating system resident in the kernel space (col.8, lines 47-62 and col.13-15).

As per claim 4: See Ellison on col.11, lines 5-15; discussing the method as claimed in claim 3, wherein the cryptographic function comprises a public/private key pair.

As per claim 5: See Ellison on col.7, lines 25-30; discussing the method as

claimed in claim 3, further comprising receiving the initial secret from a system administrator.

As per claim 8:

Ellison discloses a data processing system comprising:

a processor; a memory connected to the processor; and (col., lines)

detection logic connected to the processor and the memory, the detection logic, in use:

providing an initial secret; (col.7, lines 25-30)

binding the initial secret (col.3, lines 52-65 and col.9, lines 4-7) to data indicative of an initial state of the system, which is installed on the kernel layer between a hardware layer and an operating system layer (col.6, line 60 – col.7, line 5 and col.8, lines 38-60), via a cryptographic function; (col.2, lines 45-55 and col.3, lines 11-20)

recording state changing administrative actions performed on the system in a log, the state changing administrative actions comprising one or more of: *[an installation of kernel modules and an alternation of system run-level codes]*; (col.10, lines 43-65)

prior to performing each state changing administrative action, generating a new secret by performing the cryptographic function on a combination of data indicative of the administrative action and the previous secret, and erasing the previous secret; (col.9, lines 10-43 and col.11, lines 40-48)

evolving the initial secret based on the log to produce an evolved secret;

comparing the evolved secret with the new secret; (col.11, lines 15-33 and 48-57)

determining that the system is uncorrupted if the comparison indicates a match between the evolved secret and the new secret; and (col.9, lines 45-55 col.11, lines 59-67)

determining that the system in corrupted if the comparison indicate a mismatch between the evolved secret and the new secret; (col.9, lines 55-60)

wherein the cryptographic function comprises a one-way hash function and the hash function comprises an exponentiation function. (col.9, lines 44-45)

Ellison teaches the invention includes an operating system with software modules such as the kernel that the processor nub loader is a protected bootstrap loader code held within a chipset in the system and records state changing administrative actions (col.3, lines 10-25). Although, Ellison suggests the protection of the operating system and kernel, however, Ellison did not clearly focus on kernel protection which fails to implicitly discuss the claimed recording state changing administrative action comprises an installation of kernel modules and an alternation of system run-level codes.

Teal teaches a system and method to verify the integrity of communications entering each individual computer resource in a computer network and thereby thwart unwanted or malicious intrusions into that portion of an independent operating system resident in the kernel space of each

computer resource in a computer network (col.1, lines 20-25 and col.3, lines 7-28). The invention includes computer code set which is loaded into the kernel where communication with which that portion of the operating system resident in the kernel space is checked by a computer code set installed in the kernel space. This is designed to detect and if necessary prevent the entry of unwanted or malicious programming code into that portion of operating system resident in the kernel space (col.8, lines 47-62). Teal further explains the operations and functions of loadable kernel modules and management of the kernel space on columns 13-15.

Therefore, it would have been obvious for a person of ordinary skills in the art to combine the teachings of Ellison with Teal to teach recording state changing administrative action comprises an installation of kernel modules and an alternation of system run-level codes because to thwart unwanted or malicious intrusions by detecting and preventing the entry of unwanted or malicious programming code into that portion of operating system resident in the kernel space (col.8, lines 47-62 and col.13-15).

As per claim 9: See Ellison on col.7, lines 43-44 and col.23, lines 20-34; discussing the system as claimed in claim 8, wherein the cryptographic function comprises a public/private key pair.

As per claim 10: See Ellison on col.7, lines 28-42***;*** discussing the system as claimed in claim 8, wherein the detection logic receives the initial secret from a system administrator.

As per claim 11: See Ellison on col. 4, lines 62-63 and col.6, lines 23-26**;** discussing a computer program element comprising computer program code means which, when loaded in a processor of a computer system, configures the processor to perform a method as claimed in claim 3.

As per claim 13: See Ellison on col.3, lines 10-27; discussing a program storage device readable by machine, tangibly embodying a program of instructions executable by the machine to perform method steps for detecting an attack on a data processing system, said method steps comprising the steps of claim 3.

As per claim 14: See Ellison on col.3, lines 10-27**;** discussing a computer program product comprising a computer usable medium having computer readable program code means embodied therein for causing a data processing system, the computer readable program code means in said computer program product comprising computer readable program code means for causing a computer to effect the functions of claim 8.

As per claim 15:

Ellison discloses a method for cryptographic entangling of state and administration in a data processing system installed on the kernel layer, the method comprising:

initializing the system, which is installed on the kernel layer between a hardware layer and an operating system layer (col.6, line 60 – col.7, line 5 and

col.8, lines 38-60), by generating an initial secret releasing binding data; (col.3, lines 52-65 and col.9, lines 4-7)

binding the binding data to the initial secret via a cryptographic function; (col.2, lines 45-55 and col.3, lines 11-20)

updating the initial secret in advance of an administrative action by computing a new secret (col.11, lines 15-33 and 48-57), the state changing administrative actions comprising one or more of: *[an installation of kernel modules and an alternation of system run-level codes]*; (col.10, lines 43-65)

erasing the initial secret together with any information from which the initial secret might be derived; (col.9, lines 10-43 and col.11, lines 40-48)

recording data indicative of the administrative action; (col.12, lines 34-67 and col.13, lines 8-42)

permitting execution of the administrative action; (col.9, lines 45-55 col.11, lines 59-67)

offering a proof that the new secret corresponds to the initial secret as it has evolved according to a record of administrative actions, (col.9, lines 55-60)

wherein the cryptographic function comprises a one-way hash function and the hash function comprises an exponentiation function. (col.9, lines 44-45)

Ellison teaches the invention includes an operating system with software modules such as the kernel that the processor nub loader is a protected bootstrap loader code held within a chipset in the system and records state

changing administrative actions (col.3, lines 10-25). Although, Ellison suggests the protection of the operating system and kernel, however, Ellison did not clearly focus on kernel protection which fails to implicitly discuss the claimed recording state changing administrative action comprises an installation of kernel modules and an alternation of system run-level codes.

Teal teaches a system and method to verify the integrity of communications entering each individual computer resource in a computer network and thereby thwart unwanted or malicious intrusions into that portion of an independent operating system resident in the kernel space of each computer resource in a computer network (col.1, lines 20-25 and col.3, lines 7-28). The invention includes computer code set which is loaded into the kernel where communication with which that portion of the operating system resident in the kernel space is checked by a computer code set installed in the kernel space. This is designed to detect and if necessary prevent the entry of unwanted or malicious programming code into that portion of operating system resident in the kernel space (col.8, lines 47-62). Teal further explains the operations and functions of loadable kernel modules and management of the kernel space on columns 13-15.

Therefore, it would have been obvious for a person of ordinary skills in the art to combine the teachings of Ellison with Teal to teach recording state changing administrative action comprises an installation of kernel modules and an alternation of system run-level codes because to thwart unwanted or

malicious intrusions by detecting and preventing the entry of unwanted or malicious programming code into that portion of operating system resident in the kernel space (col.8, lines 47-62 and col.13-15).

As per claim 16: as rejected in claim 15; discussing a method as recited in claim 15, wherein the step of offering retrieves the initial secret via a request for entry of the initial secret by a system administrator, retrieving the record of administrative actions previous stored; and evolving a candidate secret for the initial secret based on the record of administrative actions retrieved; comparing the candidate secret with a current secret; if the candidate secret matches the current secret, reporting that the data processing system is still in an uncorrupted state, and if the candidate secret does not match the current secret, reporting that the data processing system is in a potentially compromised state.

As per claim 17: See Teal on col.8, lines 47-62 and col.13-15; discussing the method as recited in claim 15, further comprising permitting detection of any Trojan horse within the system.

As per claim 18: See Ellison on col.7, lines 5-20; discussing the method as recited in claim 15, wherein the initial secret is supplied via a secure communication channel.

As per claim 19: See Ellison on col.6, line 60 – col.7, line 5 and col.8, lines 38-60; discussing the method as recited in claim 15, wherein the binding data takes different forms depending on the data processing system, an application

of the data processing system, and a trust mechanisms associated with communication of the initial secret.

As per claim 20: See Ellison on col.10, lines 43-65 and col.12, lines 35-60; discussing the method as recited in claim 15, wherein the administrative action is an action taken from a group of actions consisting of: updating of system executable code; updating of system libraries; installation of kernel modules; reading of files such as those used to store system states during rebooting operations; alteration of configuration files; alteration of system run-level codes; writing to or reading from peripheral devices; and any combination of these actions.

As per claim 20: See Ellison on col.11, lines 10-65 and col.12, lines 35-60***;*** discussing a method as recited in claim 15, wherein the step of computing the new secret includes applying a one way function to a combination of a previous secret and data indicative of the administrative action.

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Leynna T. Truvan whose telephone number is (571) 272-3851. The examiner can normally be reached on Monday - Thursday (7:00 - 5:00PM).

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kim Vu can be reached on (571) 272-3859. The fax

phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/L. T. T./
Examiner, Art Unit 2135
/KimYen Vu/
Supervisory Patent Examiner, Art Unit 2135